IN THE CLAIMS:

Amended claims follow:

1. (Currently Amended) A method of scanning a communication received at a firewall for target content, wherein the communication is directed to one of a set of computer nodes connected to the firewall, comprising:

maintaining on the firewall a scanning module configured to scan communications received at the firewall;

maintaining a set of criteria for determining when one of said communications may be scanned at a computer node connected to the firewall instead of at the firewall;

partitioning responsibility for scanning said communications between said firewall and a first computer node connected to the firewall;

receiving a first communication at the firewall, wherein said first communication is intended for said first computer node;

identifying one or more attributes of said first communication;

determining from said criteria and said attributes whether to scan said first communication for target content on the firewall;

determining from said criteria and said attributes whether said first computer node is configured to scan said first communication for said target content; and

forwarding said first communication to said first computer node;

wherein said first computer node receives and scans the communication for said target content;

wherein said partitioning comprises:

receiving scanning capabilities of a first computer node connected to the firewall;

consulting a set of scanning requirements specified by an operator of the firewall; and

specifying a set of criteria to identify when a communication may be scanned for target content by said first computer node.

2. (Original) The method of claim 1, further comprising:

receiving a second communication at the firewall, wherein said second communication is intended for a second computer node;

identifying one or more attributes of said second communication;

determining from said criteria and said attributes of said second communication whether said second computer node is permitted to scan said second communication for predetermined content;

scanning said second communication at the firewall for said predetermined content; and

forwarding said second communication to said second computer node;

wherein said second computer node receives but does not scan said second communication for said predetermined content.

3. (Currently Amended) ~~The method of claim 2, further comprising:~~A method of scanning a communication received at a firewall for target content, wherein the communication is directed to one of a set of computer nodes connected to the firewall, comprising:

maintaining on the firewall a scanning module configured to scan communications received at the firewall;

maintaining a set of criteria for determining when one of said communications may be scanned at a computer node connected to the firewall instead of at the firewall;

partitioning responsibility for scanning said communications between said firewall and a first computer node connected to the firewall;

receiving a first communication at the firewall, wherein said first communication is intended for said first computer node;

identifying one or more attributes of said first communication;

determining from said criteria and said attributes whether to scan said first communication for target content on the firewall;

determining from said criteria and said attributes whether said first computer node is configured to scan said first communication for said target content;

forwarding said first communication to said first computer node; wherein said first computer node receives and scans the communication for said target content;

receiving a second communication at the firewall, wherein said second communication is intended for a second computer node;

identifying one or more attributes of said second communication;

determining from said criteria and said attributes of said second communication whether said second computer node is permitted to scan said second communication for predetermined content;

scanning said second communication at the firewall for said predetermined content;

forwarding said second communication to said second computer node; and

marking said second communication before said forwarding to said second computer node;

wherein said first computer node receives and scans the communication for said target content.

4. (Cancelled)

5. (Currently Amended) The method of claim [4]1, wherein said partitioning further comprises receiving a set of proposed criteria from said first computer node.

6. (Currently Amended) ~~The method of claim 1,~~A method of scanning a communication received at a firewall for target content, wherein the communication is directed to one of a set of computer nodes connected to the firewall, comprising:

maintaining on the firewall a scanning module configured to scan communications received at the firewall;

maintaining a set of criteria for determining when one of said communications may be scanned at a computer node connected to the firewall instead of at the firewall;

partitioning responsibility for scanning said communications between said firewall and a first computer node connected to the firewall;

receiving a first communication at the firewall, wherein said first communication is intended for said first computer node;

identifying one or more attributes of said first communication;

determining from said criteria and said attributes whether to scan said first communication for target content on the firewall;

determining from said criteria and said attributes whether said first computer node is configured to scan said first communication for said target content; and

forwarding said first communication to said first computer node;

wherein said first computer node receives and scans the communication for said target content;

wherein said determining comprises:

identifying whether said firewall is capable of scanning said first communication for target content;

determining whether said firewall is configured to share responsibility for scanning said communications with one or more of said plurality of computer nodes;

determining whether said first node is capable of scanning said first communication for said target content; and

determining whether said communication satisfies one or more criteria in said set of criteria.

7. (Currently Amended) A method of protecting a network of computer nodes from computer viruses, wherein the network of computer nodes is connected to a firewall, comprising:

maintaining a set of scanning rules for determining when a communication received at a firewall is to be scanned on the firewall and

when said communication may be scanned by the destination node of said communication;

receiving a first communication at the firewall, wherein said first communication is intended for a first computer node connected to the firewall;

determining whether a first virus scanner is enabled on the firewall;

determining whether a second virus scanner is enabled on said first computer node;

identifying a first set of attributes of said first communication;

determining from said first set of attributes and said rules that said first communication is to be scanned on said first computer node;

forwarding said first communication to said first computer node without scanning said first communication for computer viruses, wherein said first computer node scans said first communication for computer viruses using said second virus scanner;

receiving a second communication at the firewall;

identifying a second set of attributes of said second communication;

determining from said second set of attributes and said rules that the firewall is responsible for scanning said first communication for computer viruses; and

operating said first virus scanner to scan said second communication for computer viruses;

wherein said set of scanning rules comprises:

a first subset of scanning rules for determining when said communication may be scanned for target content by a destination node of said communication instead of the firewall; and

a second subset of scanning rules for determining when said communication is to be scanned on said destination node and not on the firewall.

8. (Currently Amended) ~~The method of claim 7,~~A method of protecting a network of computer nodes from computer viruses, wherein the network of computer nodes is connected to a firewall, comprising:

maintaining a set of scanning rules for determining when a communication received at a firewall is to be scanned on the firewall and when said communication may be scanned by the destination node of said communication;

receiving a first communication at the firewall, wherein said first communication is intended for a first computer node connected to the firewall;

determining whether a first virus scanner is enabled on the firewall;

determining whether a second virus scanner is enabled on said first computer node;

identifying a first set of attributes of said first communication;

determining from said first set of attributes and said rules that said first communication is to be scanned on said first computer node;

forwarding said first communication to said first computer node without scanning said first communication for computer viruses, wherein said first computer node scans said first communication for computer viruses using said second virus scanner;

receiving a second communication at the firewall;

identifying a second set of attributes of said second communication;

determining from said second set of attributes and said rules that the firewall is responsible for scanning said first communication for computer viruses; and

operating said first virus scanner to scan said second communication for computer viruses;

wherein said set of scanning rules comprises:

a first subset of firewall rules for application by the firewall to determine how to handle said communication; and

a second subset of proxy rules for application by a proxy operating on the firewall to determine how to handle said communication.

9. (Cancelled)

10. (Currently Amended) The method of claim [9]7, further comprising negotiating between the firewall and said first node to define said first subset of said scanning rules.

11. (Currently Amended) The method of claim [9]7, further comprising receiving said second subset of said scanning rules from a firewall administrator.

12. (Original) The method of claim 10, wherein said negotiating comprises:

establishing a secure connection between the firewall and said first node;

receiving at the firewall a proposed set of criteria for determining when said first node shall scan a communication instead of the firewall; and

determining whether said proposed set of criteria conflicts with said second subset of said scanning rules.

13. (Original) The method of claim 10, wherein said negotiating further comprises providing said first subset of said scanning rules to said first node.

14. (Original) The method of claim 10, wherein said negotiating further comprises sending an updated version of said second virus scanner to said first node.

15. (Original) The method of claim 10, wherein said negotiating is performed after said second virus scanner is configured on said first node by a user.

16. (Original) The method of claim 10, wherein said negotiating is performed after said first node is rebooted.

17. (Currently Amended) A computer readable storage medium storing instructions that, when executed by a computer, cause the computer to

perform a method of scanning a communication received at a firewall for target content, wherein the communication is directed to one of a set of computer nodes connected to the firewall, the method comprising:

maintaining on the firewall a scanning module configured to scan communications received at the firewall;

maintaining a set of criteria for determining when one of said communications may be scanned at a computer node connected to the firewall instead of at the firewall;

partitioning responsibility for scanning said communications between said firewall and a first computer node connected to the firewall;

receiving a first communication at the firewall, wherein said first communication is intended for said first computer node;

identifying one or more attributes of said first communication;

determining from said criteria and said attributes whether to scan said first communication for target content on the firewall;

determining from said criteria and said attributes whether said first computer node is configured to scan said first communication for said target content; and

forwarding said first communication to said first computer node;

wherein said first computer node receives and scans the communication for said target content;

wherein said partitioning comprises:

receiving scanning capabilities of a first computer node connected to the firewall;

consulting a set of scanning requirements specified by an operator of the firewall; and

specifying a set of criteria to identify when a communication may be scanned for target content by said first computer node.

18.-22. (Cancelled)